Using Innovative Instructions to Create Trustworthy Software Solutions

Matthew Hoekstra (matthew.hoekstra@intel.com)
Reshma Lal (reshma.lal@intel.com)
Pradeep Pappachan (pradeep.m.pappachan@intel.com)
Vinay Phegade (vinay.phegade@intel.com)
Juan Del Cuvillo (juan.b.del.cuvillo@intel.com)

Abstract Overview:
Software developers face a number of challenges when creating applications that attempt to keep important data confidential. Even with diligent attention paid to correct software design and implementation practices, secrets can still be exposed through a single flaw in any of the privileged code on the platform, code which may have been written by thousands of developers from hundreds of organizations throughout the world. Intel is developing innovative security technology which provides the ability for software developers to maintain control of the security of sensitive code and data by creating trusted domains within applications to protect critical information during execution and at rest. This paper will describe how this technology has been effectively used in lab exercises to protect private information in applications including enterprise rights management, video chat, trusted financial transactions, and others. Examples will include both protection of local processing and the establishment of secure communication with cloud services. It will illustrate useful software design patterns that can be followed to create many additional types of trusted software solutions.

HASP '13, Jun 23-24 2013, Tel-Aviv, Israel
ACM 978-1-4503-2118-1/13/06.